Foundation of Cryptography, Spring 2014 | Iftach Haitner

Problem set 1

March 4, 2014 | Due: March 18

- Please submit the handout in class, or email me, in case you write in LaTeX
- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a "solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- In it ok to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write his solution by *himself* (joint effort is only allowed in the "thinking phase")
- The notation we use appear in the introduction part of the first lecture (*Notation* section).

1. Let P and Q be distributions over a finite set $\mathcal{U}$.
   (a) Prove that $\mathrm{SD}(P,Q) = \max_{\mathcal{S}\subseteq\mathcal{U}}(P(\mathcal{S})-Q(\mathcal{S}))$ (recall that $\mathrm{SD}(P,Q) := \frac{1}{2}\sum_{u\in\mathcal{U}}|P(u)-Q(u)|$).
   (b) Use (a) to prove that $\mathrm{SD}(P,Q) = \max_{\mathsf{D}}\{\Pr_{x\leftarrow P}[\mathsf{D}(x)=1] - \Pr_{x\leftarrow Q}[\mathsf{D}(x)=1]\}$, where the max is take *over* all deterministic algorithms.[1]

2. Let $\mathbb{Q} = \{Q_n\}_{n\in\mathbb{N}}$, $\mathcal{P} = \{P_n\}_{n\in\mathbb{N}}$ and $\mathcal{R} = \{R_n\}_{n\in\mathbb{N}}$ be distribution ensembles.
   (a) Given that $\mathbb{Q} \stackrel{c}{\equiv} \mathcal{P}$ (i.e., $\mathbb{Q}$ is computationally indistinguishable from $\mathcal{P}$) and $\mathcal{P} \stackrel{c}{\equiv} \mathcal{R}$, prove that $\mathbb{Q} \stackrel{c}{\equiv} \mathcal{R}$.
   (b) Give an example for ensemble $\mathbb{Q}$ and $\mathcal{P}$ such that:
      i. $\mathrm{Supp}(Q_n) = \mathrm{Supp}(P_n)$ for every $n \in \mathbb{N}$, and
      ii. $\mathrm{SD}(Q_n, P_n) = 1 - \mathrm{neg}(n)$; i.e., $\forall p \in \mathrm{poly}$, $\exists n' \in \mathbb{N}$ such that $\mathrm{SD}(Q_n, P_n) > 1 - \frac{1}{p(n)}$ for every $n > n'$.

3. Refute the following conjecture:

   For every length-preserving one-way function f, the function $f'(x) = f(x) \oplus x$ is one-way.

4. Prove that the existence of pseudorandom generators implies the existence of one-way functions.

5. (a) Let $\{X_n, Z_n\}_{n\in\mathbb{N}}$ be distribution ensemble, where $\mathrm{Supp}(X_n) = \{0,1\}$ and $\mathrm{Supp}(Z_n) = \{0,1\}^n$ (i.e., X_n is a bit and Z_n is an n-bit string). Assume there exists a PPT A, function $\varepsilon\colon \mathbb{N} \mapsto [0,1]$ and set $\mathcal{I} \subseteq \mathbb{N}$, such that
   $$\Pr[\mathsf{A}(Z_n) = X_n] \geq \frac{1}{2} + \varepsilon(n)$$
   for every $n \in \mathcal{I}$. Prove there exists PPT B such that
   $$\Pr[\mathsf{B}(Z_n, X_n) = 1] - \Pr[\mathsf{B}(Z_n, U_1) = 1] \geq \varepsilon(n)$$
   for every $n \in \mathcal{I}$, where U_1 is uniformly distributed over $\{0,1\}$ (independently, of (X_n, Z_n).
   (b) Use (a) to show that if b is *not* an hardcore predicate of $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, then $(f(U_n), b(U_n))$ is computationally *distinguishable* from $(f(U_n), b(U_1))$ — there exists a PPT that distinguishes between $\{\{(f(x), b(x))\}_{x\leftarrow\{0,1\}^n}\}_{n\in\mathbb{N}}$ and $\{\{(f(x), c)\}_{x\leftarrow\{0,1\}^n, c\leftarrow\{0,1\}}\}_{n\in\mathbb{N}}$ with $1/p(n)$ advantage, for some $p \in \mathrm{poly}$, for infinitely many n's.

6. Let f be a one-way function. Prove that for any PPT A, it holds that
   $$\Pr_{x\leftarrow\{0,1\}^n, i\leftarrow[n]}[\mathsf{A}(f(x), i) = x_i] \leq 1 - \frac{1}{2n},$$
   for large enough $n \in \mathbb{N}$, where x_i is the i'th bit of x.

   Bonus* : prove the above when replacing the term $1 - \frac{1}{2n}$ with $1 - \frac{1}{n}$.

[1] The statement holds also for randomized algorithms, but require an additional step.